

SYSTEM AND METHOD FOR PROVIDING SECURITY  
IN A TELECOMMUNICATION NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is filed concurrently with the following commonly-owned applications:

5 SYSTEM AND METHOD FOR MAINTAINING A COMMUNICATION LINK,  
Attorney Docket 062891.0293;

SYSTEM AND METHOD FOR ENABLING MULTICAST  
TELECOMMUNICATIONS, Attorney Docket 062891.0297; and

10 SYSTEM AND METHOD FOR A VIRTUAL TELEPHONY INTERMEDIARY,  
Attorney Docket 062891.0381.

TECHNICAL FIELD OF THE INVENTION

15 This invention relates generally to the field of telecommunications, and more specifically to a system and method for providing security in a telecommunication network.

BACKGROUND OF THE INVENTION

Historically, telecommunications have involved the transmission of voice and fax signals over a network dedicated to telecommunications, such as the Public Switched Telephone Network (PSTN) or a Private Branch Exchange (PBX). Similarly, data communications between computers have also historically been transmitted on a dedicated data network, such as a local area network (LAN) or a wide area network (WAN). Currently, telecommunications and data transmissions are being merged into an integrated communication network using technologies such as Voice over Internet Protocol (VoIP).

Since many LANs and WANs transmit computer data using Internet Protocol (IP), VoIP uses this existing technology to transmit voice and fax signals by converting these signals into digital data and encapsulating the data for transmission over an IP network. Furthermore, by using existing "long distance" computer networks, such as private (or leased) WANs or the Internet, telephone calls can be made to distant locations using VoIP without incurring long distance telephone charges. For example, an employee of a company in Dallas can call a co-worker who is based in San Jose using the company's existing WAN. However, if these long distance communications are made over untrusted networks, or if calls are received from untrusted locations, security problems arise. These security issues exist when using VoIP since the IP telephones are connected to the same networks as computers containing sensitive information.

SUMMARY OF THE INVENTION

In accordance with the present invention, a system and method for providing security in a telecommunication network are provided that substantially eliminate or reduce disadvantages or problems associated with previously developed systems and methods. In particular, the present invention contemplates an authentication controller capable of evaluating incoming telecommunications, and a telephony proxy capable of serving as an intermediary to enable a telephone call between a trusted telephone and an untrusted device.

In one embodiment of the present invention, a method is provided for establishing a telephone call between a trusted Internet Protocol (IP) telephone and an untrusted device. The method includes receiving a call initiation request from the untrusted device that indicates a desired communication with the trusted IP telephone. The method evaluates the call initiation request, and establishes a telecommunication link between the untrusted device and the trusted telephone in response to a positive evaluation of the call initiation request.

In another embodiment of the present invention, a communication network is provided for establishing a telephone call between a trusted telephone and an untrusted device. The communication network includes a first trusted network and a trusted telephone coupled to the first trusted network. The communication network also includes an authentication controller coupled to the first trusted network and operable to evaluate a call initiation request received from an untrusted device external to the first trusted network. The call initiation request indicates a

desired communication with the trusted telephone. The network further includes a call manager operable to initiate the creation of a telecommunication link between the trusted telephone and the untrusted device in response to a positive evaluation of the call initiation request.

Technical advantages of the present invention include a system and method for providing security in a telecommunication network. The present invention allows telecommunications between a trusted telephone coupled to a protected network and an untrusted device external to the protected network to occur while still maintaining network security. The present invention can be used to evaluate incoming telecommunications based on a number of factors, including, but not limited to, the source and/or destination of the telecommunications, the transmission format of the telecommunications, and the compression format of the telecommunications.

The present invention may also provide a telephony proxy that serves as an intermediary between the trusted telephone and the untrusted device. The telephony proxy can be implemented in various forms, such as software or embedded firmware for incorporation into hardware such as routers and firewalls. The telephony proxy may also be used to manipulate the media streaming between the trusted telephone and the untrusted device as required to maintain the integrity of the protected network. Other technical advantages are readily apparent to one skilled in the art from the following figures, descriptions, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, and for further features and advantages, reference is now made to the following description, taken  
5 in conjunction with the accompanying drawings, in which:

FIGURE 1 illustrates an exemplary communication network in accordance with the present invention;

FIGURE 2 illustrates an exemplary telecommunication link between network devices using a virtual telephony device in accordance with the present invention; and  
10

FIGURE 3 illustrates an exemplary method for establishing a telephone call between a trusted telephone and an untrusted device in the communication network of FIGURE 1.

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 illustrates an exemplary communication network 10. In the illustrated embodiment, communication network 10 includes a plurality of local area networks (LANs) 20, 30, 40 that are interconnected using various techniques, including the Internet 50 and a wide area network (WAN) 60. Each LAN is a computer data network that is further operable to transmit audio and/or video telecommunication signals. Communication network 10 also includes a remote communication site 70 coupled to one or more of LANs 20, 30, 40 using the Public Switched Telephone Network (PSTN) 80. Although a specific communication network is illustrated in FIGURE 1, the term "communication network" should be interpreted as generically defining any network or combination of networks capable of transmitting telecommunication signals, data, and/or messages.

In a particular embodiment, LANs 20, 30, 40 are Ethernet networks that transmit data using the Internet Protocol (IP). However, LANs 20, 30, 40 may be any type of network that allows the transmission of audio and/or video telecommunication data, as well as traditional computer data. Therefore, although subsequent description will be primarily focused on IP networks, it should be understood that other appropriate networks including, but not limited to, Frame Relay networks, Asynchronous Transfer Mode networks, and Token Ring networks are also included within the scope of this description.

As mentioned above, LANs 20, 30, 40 are coupled to each other using other IP networks. For example, LAN 20 is coupled to LAN 30 using Internet 50, which is a public IP network. Similarly, LAN 20 is coupled to LAN 40 through WAN

60, which is typically a semi-private IP network (such as a set of communications lines owned by a telecommunication company and leased to various businesses). Remote site 70 may be coupled with LANs 20, 30, 40 using Internet 50 and/or PSTN 80. Remote site 70 may be directly connected to Internet 50, or it may use PSTN 80 to send data to and receive data from Internet 50 using an Internet Service Provider (ISP) 90. Furthermore, remote site 70 may be coupled to a LAN, such as LAN 20, using only PSTN 80. In this case, a gateway 22 facilitates communications between telephony devices at remote site 70 and LAN 20 by converting between the different data transmission formats (e.g., audio compression and encoding formats) utilized by LAN 20 and PSTN 80.

IP networks transmit data (including voice and video data) by placing the data in packets and sending each packet to the selected destination. Unlike a circuit-switched network (e.g., PSTN 80), dedicated bandwidth is not required for the duration of a call or fax transmission over LANs 20, 30, 40, Internet 50 or WAN 60. Instead, each network device sends packets across the network as they become available for transmission. This feature makes bandwidth available for other transmissions when voice or fax data is not being transmitted.

IP telephony devices, such as an IP telephone, can be coupled to any of these IP networks and used for communication between users of the networks. Furthermore, since all IP networks share a common method of transmitting data, telecommunication signals may be transmitted between telephony devices that are located on different, but interconnected, IP networks. The technology that allows

telecommunications to be transmitted over an IP network may be referred to as Voice over IP (VoIP). As an example, IP telephony devices 24 are coupled to LAN 20 to allow communication over LAN 20. IP telephony devices 24 have the capability of encapsulating a user's voice (or other inputs, such as the user's image) into IP packets so that the voice can be transmitted over LANs 20, 30, 40, Internet 50, WAN 60, and/or PSTN 80. IP telephony devices may include telephones, fax machines, computers running telephony software (such as MICROSOFT NETMEETING), gateways, or any other device capable of performing telephony functions over an IP network. For the purposes of this application, all types of telephony devices (both IP and non-IP) will be referred to as "telephones."

One example of an IP telephone is an IP Ethernet telephone that plugs directly into an Ethernet RJ-45 jack, as opposed to a traditional RJ-11 telephone jack. Alternatively, a user may plug a handset or headset directly into a personal computer on an IP network to form a virtual IP telephone. An IP telephone typically resembles a traditional digital PBX telephone, but instead of connecting to a proprietary PBX port, the telephone has an IP port, such as an Ethernet port. An IP telephone operates as a standard IP network device and typically has its own IP address (IP telephones may also have more than one IP address). IP telephones may also have the ability to handle data coding and decoding at the telephone. This feature allows the telephone to switch compression schemes on demand, such as switching between G.711 and G.723 compression.

A call manager 26 controls IP telephones 24 on LAN 20.



Call manager 26 is an application that controls call processing, routing, telephone features and options (such as call hold, call transfer and caller ID), device configuration, and other telephony functions and parameters within communication network 10. Call manager 26 can control all of the IP telephones 24 on LAN 20, and it may also control IP telephones on other IP networks. For example, call manager 26 is capable of controlling IP telephones 32 on LAN 30 and IP telephones 42 on LAN 40.

When a user wishes to place a call from an IP telephone 24a on LAN 20 to another IP telephone 24b on LAN 20 (an intra-LAN call), the calling telephone transmits a signal to call manager 26 indicating the desired function and the telephone to be called. Call manager 26 then checks on the availability of the called telephone and, if available, establishes the call by instructing the calling (originating) telephone to begin audio and/or video (media) streaming to the called (destination) telephone. The initial signaling between call manager 26 and either the originating telephone or the destination telephone is transmitted over LAN 20 using the Transmission Control Protocol (TCP). The TCP network layer in the transmitting telephone divides the data to be transmitted into one or more packets, numbers the packets, and then forwards them to the IP network layer for transmission to the destination telephone. Although each packet has the same destination IP address, the packets may travel along different paths to reach the intended destination. As the packets reach the destination telephone, the TCP layer of the destination telephone reassembles the individual packets and ensures that they all have arrived. Once TCP reassembles the data,

it forwards the data to the destination telephone as a single message.

After call manager 26 initiates the call with signaling via TCP, audio streaming between the telephones begins. A codec (coder/decoder) converts the voice, video or fax signals generated by the users of the telephones from analog voice signals into digital form. The codec may be implemented either in software or as special-purpose hardware in IP telephones 24. In the case of an IP telephone, as the user speaks into the handset, the codec converts the analog voice signals into digital data. The digitally encoded data is then encapsulated into IP packets so that it can be transmitted over LAN 20.

The encapsulation of audio and video streams between IP telephones 24 may be performed using Real-Time Transport Protocol (RTP) running over User Datagram Protocol (UDP), or any other suitable communication protocol. As with TCP, UDP uses the Internet Protocol to get data packets from one computer to another. Unlike TCP, however, UDP does not provide sequencing and error-checking of the arriving packets. However, since UDP does not perform these functions, UDP operates faster than TCP and is useful when speed is more important than accuracy. This is true of audio and video streaming since it is critical that the data be transmitted as quickly as possible, but it is not critical that every single packet is reassembled correctly (either its absence is negligible or its content can be extrapolated by the destination telephone).

Once the UDP network layer has received and reassembled the IP packets at the destination telephone, a codec in the destination telephone translates the digital

data into analog audio and/or video signals for presentation to the user. The codec may be implemented either in software or as special-purpose hardware in IP telephones 24. The entire process is repeated each time  
5 that any call participant (or any other source) generates an audio, video, or fax signal.

In addition to intra-LAN telephone calls, calls can also be placed to and received from non-IP telephones that are connected to PSTN 80, such as telephone 74 located at  
10 remote site 70. Such calls are made through gateway 22. Gateway 22 converts analog or digital circuit-switched data transmitted by PSTN 80 to packetized data transmitted by LAN 20, and vice-versa. When voice data packets are transmitted from LAN 20 to remote site 70 over PSTN 80,  
15 gateway 22 retrieves the data contained in the packets coming from LAN 20 and converts this digital data to the analog or digital format used by the PSTN trunk 82 to which gateway 22 is coupled. Since the digital format used for voice transmissions over an IP network is often different  
20 than the format used on the digital trunks of PSTN 80, the gateway provides conversion between these different digital formats, referred to as transcoding. Gateway 22 also translates between the VoIP call control system and the Signaling System 7 (SS7) protocol or other signaling  
25 protocols used in PSTN 80.

For voice transmissions from remote site 70 back to LAN 20 over PSTN 80, the process is reversed. Gateway 22 takes the incoming voice transmission (in either analog or digital form) and converts it into the digital format used  
30 by LAN 20. The digital data is then encapsulated into IP packets and transmitted over LAN 20. This process is

continued between PSTN 80 and LAN 20 through gateway 22 until the call is complete.

Remote site 70 may also include an IP telephone 72. A call may be placed between telephone 72 and another IP telephone 24 on LAN 20 using Internet 50 and ISP 90. Telephone 72 is connected to a computer 76 that is coupled to ISP 90 using a modem. IP-encapsulated audio and/or video data packets are sent from telephone 72 to computer 76. Computer 76 then uses the modem to transmit the data over PSTN to ISP 90, where the data is transmitted to Internet 50 (alternatively, computer 76 may be directly connected to Internet 50). The data is finally transmitted over Internet 50 to LAN 20, where it is received by telephone 24. Note that no gateway 22 is required, since the communication is between two IP telephones (even though the telephones are not directly connected).

Calls can also be made between an IP telephone located on LAN 20 and an IP telephone located on another LAN 30, 40, on Internet 50, or on WAN 60. For example, a call may be placed between IP telephone 24 connected to LAN 20 and IP telephone 42 connected to LAN 40. As discussed above, the analog voice or fax data is digitized and encapsulated into IP packets at the originating IP telephone 24. A router (or other similar device) then directs the packets over WAN 60 to the IP address of the destination IP telephone 42. IP telephone 42 then retrieves the data and converts it to analog form for presentation to the user. IP telephone 42 may be controlled by the same call manager 26 as IP telephone 24, or it may be controlled by a call manager on LAN 30 or LAN 40.

In any of the above scenarios, when a call is placed

to an IP telephone, for example IP telephone 24, a call initiation request is first sent to call manager 26. If the originating telephone is an IP telephone (e.g., a telephone on LAN 30, LAN 40, Internet 50, or WAN 60), the originating IP telephone generates the call initiation request and sends the request to call manager 26. If the originating telephone is a non-IP telephone, such as telephone 74, gateway 22 first intercepts the incoming call from PSTN 80, and then sends a call initiation request to call manager 26 indicating the IP telephone that is being called. In either case, once call manager 26 receives the call initiation request, call manager 26 sends a signal to the destination IP telephone offering the call to the telephone.

If the destination telephone, for example, IP telephone 24, can accept the call (e.g., it is not in use or under a Do Not Disturb instruction from the user), IP telephone 24 replies to call manager 26 that it will accept. Upon receiving this acceptance, call manager 26 transmits a signal to IP telephone 24 to cause it to ring. The telephone's user can then hear the ring and can take the telephone "off-hook" to receive the call. Taking the telephone off-hook may include, but is not limited to, picking up a handset, pressing the ringing line's button, pressing a speakerphone button, or otherwise indicating that the telephone is ready to receive the incoming call. For the purposes of this application, the term "off-hook" is used to generically indicate a condition of a telephone when it is ready to initiate or receive telecommunication signals. Once IP telephone 24 has been taken off-hook, call manager 26 establishes media streaming (such as RTP media streaming) between IP telephone 24 and the originating

telephone. If the originating telephone is a non-IP telephone, such as telephone 74, the media streaming occurs between IP telephone 24 and gateway 22. Gateway 22 then transmits the audio and/or video data to telephone 74.

5           One advantage associated with IP telephones is their ability to communicate and interact with any other IP device coupled to the IP network. For example, IP telephones may interact and communicate with other IP telephones, with non-telephony IP devices, and even with  
10       virtual telephony devices. A virtual telephony device may be implemented as software, firmware and/or hardware to interact with devices in communication network 10. Virtual telephony devices may be implemented as software or  
15       firmware on any existing or dedicated device on the IP network. For example, computer 27 contains software for implementing one or more virtual telephony devices 28. Virtual telephony device software may also be located at  
20       call manager 26, or any other network device. The computer or other device on which the virtual telephony software is located includes a network interface, a memory to store the software, and a processor to execute the software.

          Virtual telephony devices 28 may be logically inserted between two or more telephones to act as an intermediary between the two telephones. Once such a relationship is  
25       established, signaling and media streaming that passes through virtual telephony device 28 may then be modified through address translation or media stream manipulation for various reasons before they are sent on to the destination device. Reasons for such modifications include  
30       duplicating streams, dynamically redirecting streams,

maintaining connections between devices, converting between data formats (e.g., A-Law to  $\mu$ -Law), and injecting media.

As will be described in the present application, one implementation of virtual telephony device 28 is as a telephony proxy to allow telecommunications between a trusted telephone coupled to a protected network, such as LAN 20, and an untrusted device external to the protected network while still maintaining network security. Through the use of an authentication controller 25, which evaluates incoming communications, the telephony proxy can be used to monitor communications directed to trusted telephones on LAN 20, for example, from untrusted devices outside of LAN 20 (e.g., telephones coupled to LAN 40 or Internet 50). The telephony proxy may also be used to manipulate the media streaming between the trusted telephone and the untrusted device as required to maintain the integrity of the protected network.

In order for a call to be placed through a virtual telephony device, for example a call placed to IP telephone 24a in LAN 20 through virtual telephony device 28, telephone 24a should be registered with virtual telephony device 28. Telephone 24a is instructed by call manager 26 to register with virtual telephony device 28 at a specified IP address and port. Telephone 24a signals virtual telephony device 28 via TCP/IP indicating that it would like to register. If virtual telephony device 28 accepts the registration request, telephone 24a sends a registration message to virtual telephony device 28 using TCP/IP. The registration message typically comprises information about the telephone such as the telephone's IP

and media access control (MAC) addresses, the type of telephone, and the codec(s) used by the telephone.

*Sub a1*

FIGURE 2 illustrates an exemplary communication link created using virtual telephony device 28. The communication link represents any connection or other coupling between two or more telephony devices that allows the telephony devices to communicate in some manner. It should also be noted that although the TCP and UDP protocols are specifically identified in the following discussion, any other suitable signaling and media transmission protocols may be used. Virtual telephony device 28 initiates this communication link by first creating a logical connection to telephone 24a. Creating this logical connection involves associating logical UDP and TCP ports of virtual telephony device 28 with telephone 24a. Virtual telephony device 28 designates a TCP port (for example, port 2000) as the signaling port of telephone 24a and designates a UDP port (for example, port 2100) as the streaming port of telephone 24a. Virtual telephony device 28 instructs call manager 26 to send all signaling directed to telephone 24a to logical port 2000 of virtual telephony device 28. Likewise, virtual telephony device 28 instructs call manager 26 to send all media streaming directed to telephone 24a from other telephones to logical port 2100 of virtual telephony device 28. Virtual telephony device 28 will automatically forward any data that is subsequently sent to these ports of virtual telephony device 28 to the IP address of telephone 24a (for example 200.50.10.1). As far as call manager 26 is concerned, telephone 24a is located at these logical ports of virtual telephony device 28.



Likewise, virtual telephony device 28 has typically designated a TCP port (for example, port 1000) as the signaling port of call manager 26 (data is typically not streamed to and from call manager 26, so a UDP port is usually not required). Virtual telephony device 28 instructs telephone 24a (as well as any other registered telephones) to send all signaling directed to call manager 26 to logical port 1000 of virtual telephony device 28.

*Sub* In operation, when a call is placed to telephone 24a by another telephone 24b (which has registered with virtual telephony device 28 in a similar manner as telephone 24a), telephone 24b initially sends a call initiation request to call manager 26 indicating a desire to communicate with telephone 24a. This call initiation request is sent by telephone 24b to port 1000 of the IP address of virtual telephony device 28 (for example, 200.50.10.30). Virtual telephony device 28 then forwards the request to call manager 26. In order to establish the call, call manager 26 sends signaling information to telephone 24a at port 2000 of the IP address of virtual telephony device 28. Virtual telephony device 28 then forwards this signaling to telephone 24a. If telephone 24a accepts the call, call manager 26 establishes audio (and possibly video) streaming between telephones 24a and 24b by signaling telephone 24b to begin streaming data to port 2100 of virtual telephony device 28, and by signaling phone 24a to begin streaming to port 3100 of virtual telephony device 28. Thus a telecommunication link is established between telephones 24a and 24b using virtual telephony device 28.

When packets are received at port 2100, virtual telephony device 28 examines the packets and notes the

source address of the data. This source address is the IP address of telephone 24b, for example 200.50.10.2, and a particular logical port of this IP address. Virtual telephony device 28 then changes the source address and port in the header of the IP packets coming from telephone 24b to the IP address and logical UDP port of virtual telephony device 28 that was associated with telephone 24b when it registered with virtual telephony device 28 (for example, 200.50.10.30, port 3100). This address modification can be performed by an address modification module of virtual telephony device 28. Virtual telephony device 28 then forwards the packets to telephone 24a (this communication may be performed by a transmission module, such as a UDP/IP stack). Since the header of each packet indicates the media streaming originated from port 3100 of virtual telephony device 28, it appears to telephone 24a that telephone 24b is actually located at this address and port.

A similar process is performed when telephone 24a returns media streaming in response to the streaming from telephone 24b. Since it believes that telephone 24b is located at port 3100 of virtual telephony device 28, telephone 24a directs its data streaming to this location. When virtual telephony device 28 receives the IP packets at port 3100 (which it has previously associated with telephone 24b), it first changes the source IP address and port in the packets' header from the actual port and IP address (200.50.10.1) of telephone 24a to port 2100 of the IP address of virtual telephony device 28. Virtual telephony device 28 then forwards the packets to telephone 24b. Since the header of each packet indicates that the

media streaming originated from port 2100 of the IP address of virtual telephony device 28, it appears to telephone 24b that telephone 24a is actually located at this address and port. All subsequent data sent between telephones 24a and  
5 24b is similarly passed through and modified by virtual telephony device 28.

Since all data that is sent between two IP telephones may be passed through virtual telephony device 28, virtual telephony device 28 can be used for other purposes in  
10 addition to the address translation function described above. For example, virtual telephony device 28 may serve as a telephony proxy to facilitate telecommunications between a "trusted device" located in the same network as the telephony proxy and an "untrusted device" located  
15 outside the network. In this case, communications between the trusted device and the untrusted device are routed through the telephony proxy after being authenticated.

For the purposes of this application the term "trusted device" will be used to indicate an IP telephone that is coupled to a protected or trusted IP network(s) being serviced by the telephony proxy, such as telephone 24b on  
20 LAN 20. The term "untrusted device" will be used to indicate an IP or non-IP device that is external to the protected IP network(s). The untrusted device may be coupled to an untrusted network, such as telephone 52 on  
25 Internet 50. Alternatively, the untrusted device may be a telephone coupled to a trusted network, such as telephone 32 on LAN 30. In this case, the telephone is untrusted to telephony proxy 28, for example, because the trusted  
30 network (LAN 30) is coupled to the protected network (LAN 20) using an untrusted network, such as Internet 50.

For simplicity, subsequent discussion will focus on telephony proxy 28, which is a type of virtual telephony device 28, being used to provide security to LAN 20. Therefore, LAN 20 is the protected (and trusted) network and telephones 24 coupled directly to LAN 20 are trusted  
5 telephones. However, it should be understood that telephony proxy 28 can be used in conjunction with any other type of network to which security needs to be provided.

Telephony proxy 28 operates like virtual telephony  
10 device 28, described in FIGURE 2, to facilitate a telephone call between two or more telephones. However, because at least one of the telephones is untrusted when telephony proxy 28 is used, an authentication step is required before a telecommunication link can be established between the  
15 telephones. This authentication step is performed by authentication controller 25. Thus, the primary difference between the telephony proxy software and the virtual telephony device software is that the telephony proxy software does not establish a telecommunication link  
20 between a trusted device and an untrusted device until authentication controller 25 approves the link.

When a call initiation request is made by an untrusted device to a trusted device (the term "trusted device" being used to indicate the target of a call initiation request  
25 before the request is authenticated), authentication controller 25 evaluates this request to determine if a telecommunication link should be established between the trusted device and the untrusted device using telephony proxy 28. Various methods of evaluating the call initiation  
30 request, such as an address look-up or a message format analysis, are described below in conjunction with FIGURE 3.

As with telephony proxy 28, authentication controller 25 may be implemented as software on any device in LAN 20. For example, the authentication software may be located on a dedicated computer, or it may be located on a computer having other purposes such as computer 26 running the call manager software or computer 27 running the telephony proxy software. In one embodiment, the call manager software, the authentication software, and the telephony proxy software may all be running on the same computer.

FIGURE 3 illustrates an exemplary method for using a virtual telephony proxy to facilitate a telephone call between a trusted device and an untrusted device. The method begins when a call initiation request is received from an untrusted device at step 102, indicating a desire to place a telephone call to a trusted device. For example, a call initiation request directed to telephone 24a may be generated by telephone 32 on LAN 30, and transmitted over Internet 50 to LAN 20. Alternatively, a call initiation request may be transmitted to LAN 20 from various other untrusted devices using WAN 60, PSTN 80, and/or ISP 90.

The call initiation request may comprise any indication that the untrusted device would like to communicate with a trusted device. LAN 20 may be configured such that all incoming call initiation requests are first directed to telephony proxy 28. Telephony proxy 28 may work in conjunction with or as part of a firewall 29 that is used to screen non-telephony data communications. In this case, incoming call initiation requests and other incoming telephony communications are directed to telephony proxy 28, and all other incoming communications are sent through firewall 29. Alternatively, incoming call initiation

requests may be sent to other initial destinations, such as call manager 26 (note that the call manager software may be running on the same computer as the telephony proxy software).

5           Once the call initiation request has been received, the request is transferred to authentication controller 25 at step 104. As described above, the authentication controller software may be running on the same computer as telephony proxy 28 and/or call manager 26, so this  
10           transferring step may simply involve passing the call initiation request between software modules on the same computer. The call initiation request is evaluated by authentication controller 25 at step 106. A variety of  
15           evaluations may be performed on the call initiation request to determine whether the request should be accepted and whether a call should be established between the untrusted device and the trusted device.

          One such evaluation involves determining whether the trusted device is a proper recipient of a telephone call from an untrusted device. This evaluation may simply  
20           involve determining whether the trusted device is actually a telephone or some other telephony device capable of receiving telephone calls. Since IP telephony allows the integration of telephones and other network devices on the  
25           same IP network, care must be taken to ensure that unauthorized parties are not able to access secured data or send unwanted data, such as a virus, to the network.

          By ensuring that the object of the call initiation request is a telephone or other telephony device, these  
30           worries are reduced. There is typically no sensitive data located on an IP telephone that an intruder could access.

Furthermore, if a virus is sent to an IP telephone after it is connected with the untrusted device, the IP telephone may simply attempt to "play" the incoming IP packets to the telephone's user. In this case, nothing will happen since the packets are not in a media format, such as an RTP stream. Also, the data in the incoming packets is not stored at the telephone (except for temporary buffering), and it is typically not accessed in a manner that would infect the telephone or the network with a virus or other unwanted data.

One way that authentication controller 25 can determine whether the trusted device is actually a telephone is by comparing the network address of the called device with the addresses on an address list 23 stored in the memory of the computer running the authentication controller software (or in the memory of any other network device). For example, the approved address list may contain the IP addresses of telephones and other telephony devices that are permitted to receive calls from untrusted devices. Alternatively, address list 23 list may contain the IP addresses of untrusted devices that are either authorized to communicate with trusted devices or that are prohibited from communicating with trusted devices. Address list 23 may contain either individual or subnet addresses.

Once authentication controller 25 has evaluated the call initiation request, it determines the appropriate action to take at step 108 based on whether the evaluation was positive or negative. If the evaluation is negative, for example, if the trusted device to which the call is directed is not actually a telephone or other proper recipient of an incoming call, then authentication

controller 25 denies the call initiation request at step 110. Once the request is denied, call manager 26 will not attempt to establish a telecommunication link between the untrusted device and the trusted device.

5           If the evaluation of the call initiation request is positive, then authentication controller 25 transmits a signal to call manager 26 authorizing a telephone call between the trusted device and the untrusted device at step 112. In response to this signal, call manager 26  
10 establishes a telecommunication link between the trusted device and the untrusted device at step 114. This telecommunication link, as described above in conjunction with FIGURE 2, may be established such that all telecommunications between the trusted device and the  
15 untrusted device are communicated through telephony proxy 28.

          Assuming that the trusted device is registered with telephony proxy 28 (as described above), call manager 26 instructs the untrusted device to begin media streaming to  
20 the logical port of telephony proxy 28 that has been associated with the trusted device. Additionally, call manager 26 instructs telephony proxy 28 to associate another of its logical ports with the untrusted device. In the manner described above, telephony proxy 28 changes the  
25 information in header of the packets incoming from the untrusted device by altering the source address and source port to the address of telephony proxy 28 and the logical port of telephony proxy 28 that was associated with the untrusted device (note that the address may be in the IP  
30 header and the port may be in the UDP or TCP header). Telephony proxy 28 then forwards the packets to the trusted



device, so that the packets appear to be sent from telephony proxy 28. A similar address translation process is performed on packets being sent from the trusted device to the untrusted device, as described above.

5           The continuous address translation by telephony proxy 28 ensures that all communications between the trusted device and the untrusted device are controlled by telephony proxy 28. Such continuous control prevents the untrusted device from determining the actual network address of the  
10           trusted device.

          In one embodiment, telephony proxy 28 also continuously monitors the media streaming between the trusted device and the untrusted device at step 315. For example, telephony proxy 28 can ensure that the media  
15           streaming is in a recognized audio encoding format, such as G.711, G.723, or G.729. Telephony proxy 28 can also ensure that the communications between the trusted device and the untrusted device are, in fact, media streaming (or more specifically, RTP media streaming). Furthermore, any other  
20           appropriate methods of evaluating the media streaming, including appropriate techniques implemented by data firewalls, may also be used to monitor any unauthorized access to a network. If telephony proxy 28 determines at  
25           any point that suspect media streaming or other transmissions are occurring, telephony proxy 28 can manipulate or terminate the data streaming between the untrusted device and the trusted device. Once the telephone  
30           call between the trusted device and the untrusted devices is completed (or once suspect transmissions are detected), the telecommunication link is terminated at step 116.

Although the present invention has been described with several embodiments, a myriad of changes, variations, alterations, transformations, and modifications may be suggested to one skilled in the art, and it is intended  
5 that the present invention encompass such changes, variations, alterations, transformations, and modifications as fall within the spirit and scope of the appended claims.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
22